PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

8

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
22171.251		

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/27352	04/10/2000	05/10/1999

International Patent Classification (IPC) or national classification and IPC
H04L29/00

Applicant
NORTEL NETWORKS LIMITED et al.

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 34 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
01/05/2001	14.01.2002

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer

Körbler, G

Telephone No. +49 89 2399 8250

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/US00/27352

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1-25	as received on	12/12/2001	with letter of	07/12/2001

Claims, No.:

16-30	as received on	12/12/2001	with letter of	07/12/2001

(claim 1-15 + 31-127 have resulted in the deletions of the claims)

Drawings, sheets:

1/26-26/26	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☒ the claims, Nos.: 1-15, 31-127

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	16-30
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	16-30
Industrial applicability (IA)	Yes:	Claims	16-30
	No:	Claims	

2. Citations and explanations
see separate sheet

Cited documents:

D1: YAIR FRANKEL ET AL: 'SECURITY ISSUES IN A CDPD WIRELESS NETWORK' IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 2, no. 4, 1 August 1995 (1995-08-01), pages 16-27, XP000517586 ISSN: 1070-9916

D2: EP-A-0 912 026 (LUCENT TECHNOLOGIES INC) 28 April 1999 (1999-04-28)

D3: JACOBS S ET AL: 'SECURITY OF CURRENT MOBILE IP SOLUTIONS' NOV. 3 - 5, 1997,NEW YORK, NY: IEEE,US, 3 November 1997 (1997-11-03), pages 1122-1128, XP000792591 ISBN: 0-7803-4250-X

D4: JORDAN F ET AL: 'SECURE MULTICAST COMMUNICATIONS USING A KEY DISTRIBUTION CENTER' PROCEEDINGS OF THE IFIP TC6 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKS AND DATA COMMUNICATION, FUNCHAL, MADEIRA ISLAND, PORTUGAL, APR. 18 - 21, 1994,AMSTERDAM, NORTH HOLLAND,NL, vol. CONF. 5, 18 April 1994 (1994-04-18), pages 367-380, XP000593303 ISBN: 0-444-81869-3

D5: RICHARD E. SMITH: 'Internet Cryptography' October 1997 (1997-10) , ADDISON-WESLEY , USA/CANADA XP002165437

D6: HARKINS,CARREL: 'The Internet Key Exchange (IKE)' NETWORK WORKING GROUP RFC 2409, INTERNET ENGINEERING TASK FORCE(IETF) STANDARDS TRACK, November 1998 (1998-11), XP002165435

D7: MAUGHAN, SCHERTLER, SCHNEIDER, TURNER: 'Network Working roup RFC 2408 Standards Track' INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL (ISAKMP), November 1998 (1998-11), XP002165436

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The present formulation of independent method claim 16 fails to meet the requirements of Art. 33(3) PCT, because the subject-matter does not involve an inventive step.

The document D3 is regarded as being the closest prior art to the subject-matter of claim 16, and discloses (the references in parentheses applying to this document):

A method of providing secure communication between a mobile node (Figure 2, MN) and a home domain (HA) using a foreign domain (FA), comprising:
transmitting a registration request from the mobile node to the home domain (page 1125, right-hand column, line 1-3),
the request comprising an identity of a user of the mobile node in encrypted form (page 1125, right-hand column, section 3, Key Management);
the home domain receiving and processing the registration request to generate a registration reply comprising one or more encryption keys for encrypting messages to be communicated between and among the mobile node, home domain, and the foreign domain (page 1126; left-hand column, section Key Management - right-hand column, line 7); and
transmitting the registration reply from the home domain to the foreign domain and the mobile node (page 1126, right-hand column, line 8 - 25).

The subject-matter of claim 16 therefore differs from the state of the art given by D3 that the request comprises network routing information in non-encrypted form.

The objective problem be solved seems to be to use Internet security techniques and to keep routing information independent and transparent.

Document D3 already discloses (Figure 5-1 and page 121, section 5.2 "As shown in Figure 5-1...") as solution that **all data is encrypted that isn't required to route packets and that the routing data is in plaintext (not encrypted).**

A skilled person therefore starting from D3 and aware of document D5, wherein routing information is not encrypted and all other data is encrypted, would arrive at the subject-matter of claim 16, without the exercise of inventive skill, in order to

solve the problem (to use Internet security techniques and to keep routing information independent and transparent), by combining these two documents.

Therefore, the essence of the alleged invention, is also already known from D3 in combination with D5.

Consequently, the features of present claim 16 not explicitly mentioned in D3 would be found by the skilled person in a most self-evident manner; they are not based on an inventive step, and claim 16 therefore fails to meet the requirements of Art. 33 (3) PCT.

2. The dependent claims 17-30 do not seem to contain any subject-matter which, in combination with the subject-matter of the claim on which they are dependent, would lead to a claim involving an inventive activity (Article 33(3) PCT). They are either derivable from the above cited documents or concern simple embodiments without inventive merit in themselves.